Progetto Modulo M5 – Maria Ludovica Tartaglia

Traccia:

Con riferimento alla figura in slide 2, rispondere ai seguenti quesiti.

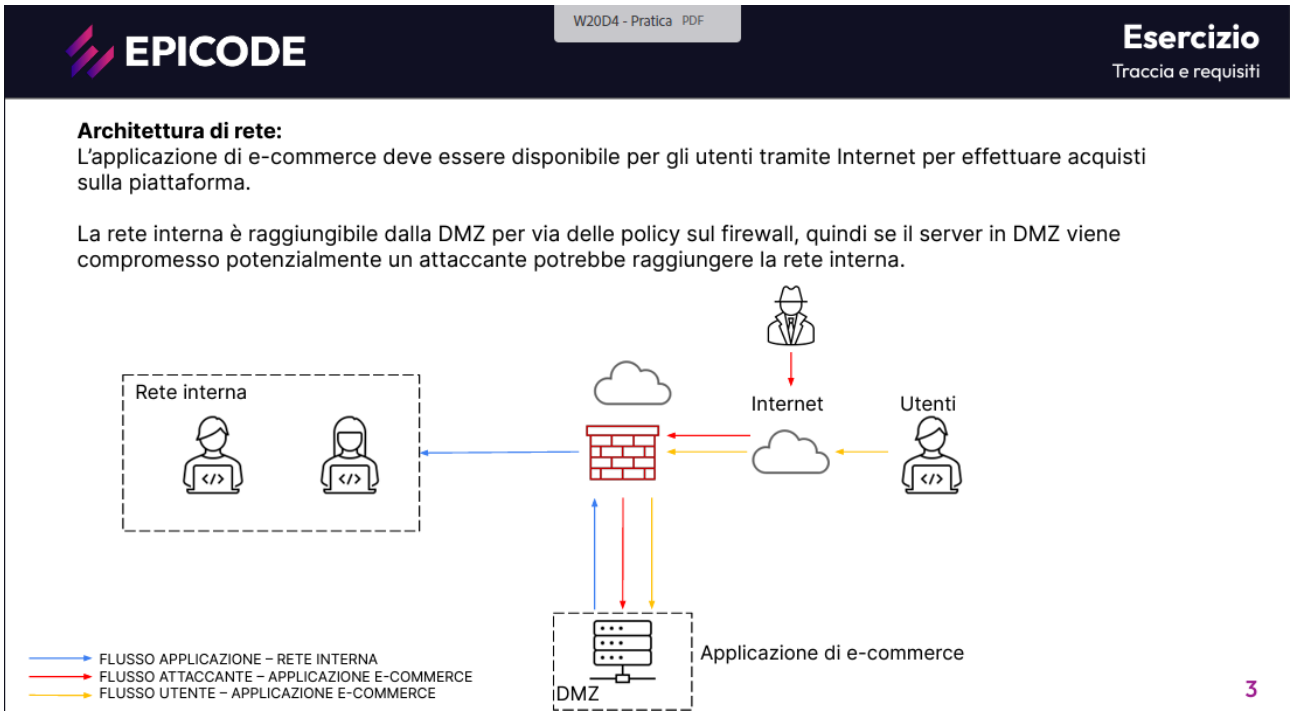
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

2. Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

3. Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)

5. Modifica "più aggressiva" dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2)



Svolgimento:

1) Per poter procedere efficacemente con delle azioni preventive che siano volte a proteggere l'applicazione web da eventuali attacchi di tipo SQL injection e Cross site-scripting (XSS), è fondamentale comprendere quali siano, a livello di sicurezza, le migliori azioni (da qui in poi "best practices") da intraprendere all'interno di un incident response. Saranno infatti molto importanti per una migliore e più efficace gestione delle minacce a cui si è costantemente esposti. Vediamo pertanto come sia possibile agire in tal senso su più fronti.
Le best practices più rilevanti per l'ottimizzazione della sicurezza informatica sono:
il **Vulnerability Assessment**; la fase di **Penetration testing**; la valutazione delle minacce, anche detta **Threat Analysis**.

   Nell'ambito del Vulnerability Assessment, sappiamo di poter utilizzare degli strumenti appositi per effettuare una scansione delle vulnerabilità presenti e correggerle; è buona pratica inoltre effettuare queste scansioni periodicamente, di modo da poter individuare tempestivamente eventuali danni al sistema e problemi di sicurezza. In questo contesto si inserisce ovviamente la prevenzione da attacchi SQL injection e XSS, procedendo ad individuare e/o prevenire l'inserimento di stringhe di codice malevolo.

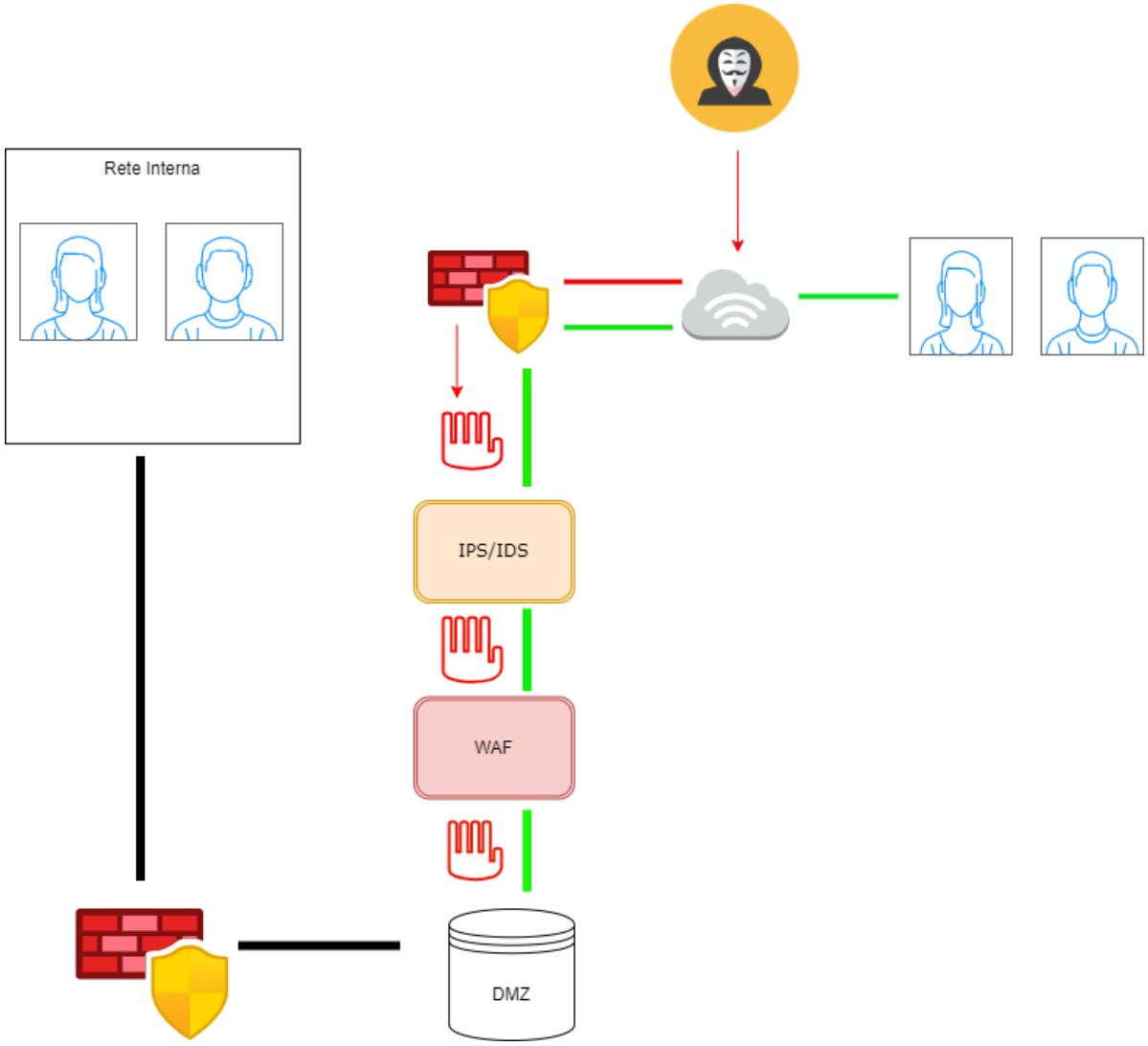
   La conduzione periodica di Penetration test è buona pratica per mantenere sempre elevata l'attenzione alla manutenzione delle misure di sicurezza. La simulazione di attacchi quali SQL injection e XSS permetterà la valutazione dell'efficacia e resistenza delle misure di sicurezza fino a quel momento adottate e l'individuazione di ipotetiche vulnerabilità non riscontrate in fase di assessment.

   Ciò premesso, andiamo a vedere nel dettaglio quali strumenti possiamo utilizzare per l'implementazione della protezione dagli attacchi informatici. Nel caso specifico proposto, vediamo un serie di azioni mirate per attacchi SQL injection e XSS.
Per prima cosa procediamo a **filtrare le connessioni in entrata**, facendo si di individuare eventuali attacchi malevoli in ingresso.

   Per fare ciò lavoreremo su due fronti:
- Filtraggio attraverso WAF (Web Application Firewall)
- Filtraggio attraverso NGFW (Next- Generation Firewall), che offre funzioni avanzate di protezione, integrando ad un normale firewall delle implementazioni avanzate che operano direttamente sull'intera rete come IPS/IDS, che monitorano gli eventi di sicurezza e prevedono azioni automatiche che fermino la potenziale intrusione.

   Possiamo inoltre avvalerci dell'utilizzo di altre due metodologie molto utili: il **SIEM** (Security Information and Event Management) per monitorare costantemente il traffico di rete ed analizzare i dati inviati da diversi dispositivi e rispondere tempestivamente a potenziali attività non consone, ed il **SDLC** (Secure Development Lifecycle) integrando la sicurezza all'interno dello sviluppo del software dall'inizio del suo ciclo vitale.

Effettueremo difatti anche dei controlli sul software stesso, di modo da individuare eventuali problematiche già esistenti (bug o simili). Per far questo, andremo ad analizzare e sanificare il codice di modo da eliminare eventuali caratteri che possano renderlo vulnerabile ad attacchi SQLi, e tecniche di reverse engineering, ove possibili in base al tipo di codice utilizzato, per poter limitare attacchi di tipo XSS.

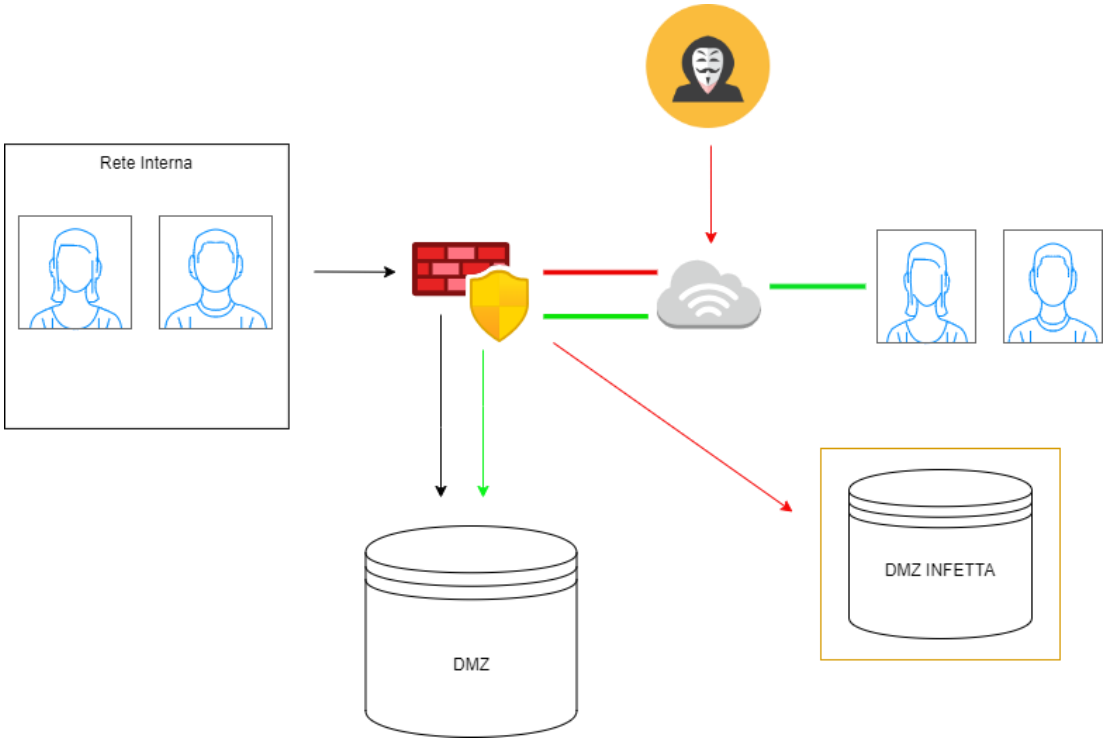


2) Per poter calcolare l'impatto sul business dovuto alla non-raggiungibilità del sito per i minuti indicati, ai costi indicati, possiamo procedere con un rapido calcolo come segue:

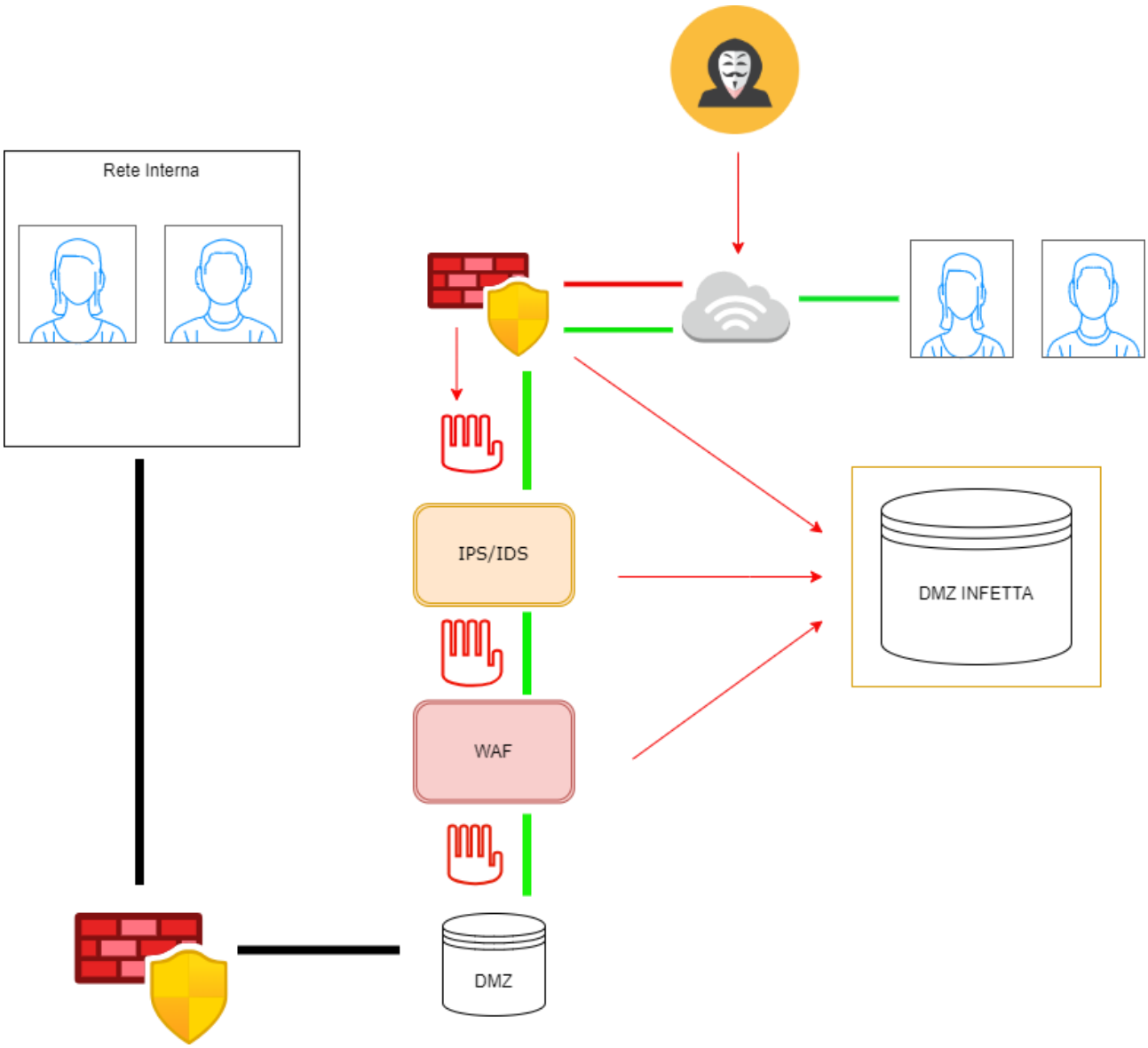
   Minuti di indisponibilità: 10 minuti
   Valore (in media) generato dagli utenti presenti sulla piattaforma e-commerce/minuto: 1.500€
   Impatto sull'attività: 10 minuti x 1.500€/minuto = 15.000€
   L'impatto che la non-raggiungibilità comporterà sull'attività nel lasso di tempo di 10 minuti sarà pertanto di 15.000€. * Bonus track: si potrebbe ipotizzare una perdita per il sito di e-commerce in termini di danno all'immagine subita, nonché per la reputazione del brand e l'insoddisfazione, e conseguente perdita, di clientela.

   Le possibili azioni preventive da esperire per evitare un impatto negativo di questo tipo sono sicuramente l'implementazione di un sistema di rilevamento e quindi prevenzione degli attacchi DDoS e l'utilizzo di un sistema di CDN (Content Delivery Network) di modo da distribuire il traffico garantendo load balancing e stemperando questa tipologia di attacchi.

3) Nella risoluzione della terza problematica, andremo ad implementare un'azione correttiva: indirizzeremo infatti il traffico dell'attaccante sul DMZ ormai già infetto, mentre gli utenti lavoreranno su un DMZ di backup. Impostando delle specifiche policy di firewall, infatti, il contenuto malevolo del malware sarà circoscritto solo al server infettato, mentre sul secondo server, quello di backup, si proseguirà normalmente attraverso le connessioni di rete interna e alle connessioni degli utenti dell'e-commerce. Le connessioni in entrata saranno pertanto indirizzate di default verso il server infetto per gli agenti del virus, e verso il server di backup per gli utenti regolarmente autorizzati.



4) Come richiesto dalla traccia, andiamo pertanto a rappresentare graficamente le azioni preventive e le soluzioni implementate nei punti 1 e 3 di cui sopra:



Come si vede, la figura mostra la nuova architettura del case scenario con tutte le modifiche apportate fino ad ora.

5) Al termine dello svolgimento della traccia, ci viene chiesto che approccio ulteriore attueremmo per modificare in maniera più “aggressiva” la nostra struttura. Sicuramente sarebbe possibile aggiungere ulteriori migliorie, come ad esempio la micro-segmentazione della rete di modo da isolarne i vari segmenti e permettere un loro maggior controllo. Altresì, è possibile pensare di spostare la web application in un ambiente di tipo cloud, in maniera da poter integrare un livello di sicurezza più elevato. Si raccomanda inoltre, come buona pratica, l’esecuzione di penetration test regolari e cadenzati nel tempo, di modo da potersi accorgere tempestivamente delle eventuali minacce e correggerle senza incorrere in problematiche. Tuttavia, un isolamento completo della rete (e conseguentemente della web application) non è una soluzione contemplabile, dal momento che renderebbe pressoché inutilizzabile il sito di e-commerce sia per gli utenti finali, ossia i clienti che intendano avvalersi del suo utilizzo, che per i dipendenti del sito stesso.